Focus on Resiliency: A Process Improvement Approach to Security

Introducing the Resiliency Engineering Framework

Rich Caralli & Lisa Young
Software Engineering Institute

CSI 33rd Annual Security Conference and Exhibition

06 November 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **06 NOV 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE **Focus on Resiliency: A Process Improvement Approach to Security Introducing the Resiliency Engineering Framework**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

CSI 33rd Annual Security Conference and Exhibition, 6-8 Nov, 2006, Orlando, FL.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**53**	

Software Engineering Institute

Established in 1984

Federally Funded Research and Development Center (FFRDC)

College-level unit of Carnegie Mellon University

Includes five technical programs aimed at helping defense, government, industry, and academic organizations to continually improve software-intensive systems

Widely-known “brands”

- CERT Coordination Center
- Capability Maturity Model Integration (CMMI)

Agenda

An evolving view of security

Operational resiliency

Embracing a process view

Introducing the Resiliency Engineering Framework

Summary and questions

A new operational environment -1

No operational boundaries

Pervasiveness of technology

Expanding and rapidly changing risk profile

High dependency on upstream partners

Successes are short-lived

Skills have shorter longevity

Less resources, more demands

A new operational environment -2

Increasing regulatory requirements

Criticality of data and information

Distributed workforce

Heightened threat level and increasing uncertainty

Insurance costs

Poses a new environment in which security must be effective and efficient

The problem with security management

Poorly planned and executed function

Business units not involved

Usually bolted on as an afterthought

Security seen as technical problem

Searching for magic bullet: CobiT, ITIL, ISO17799

Poorly defined and measured goals

Funding model reactive, not strategic

Not connected to continuity of operations planning

Organizational impact

False sense of accomplishment

Misalignment of operational and security goals

Reinforcement of silos

Less-than-resilient assets, processes, services

Misalignment with business objectives

Wasted human and financial resources

Compliance at the expense of effectiveness

Failure to manage operational risk

An evolving view of security -1

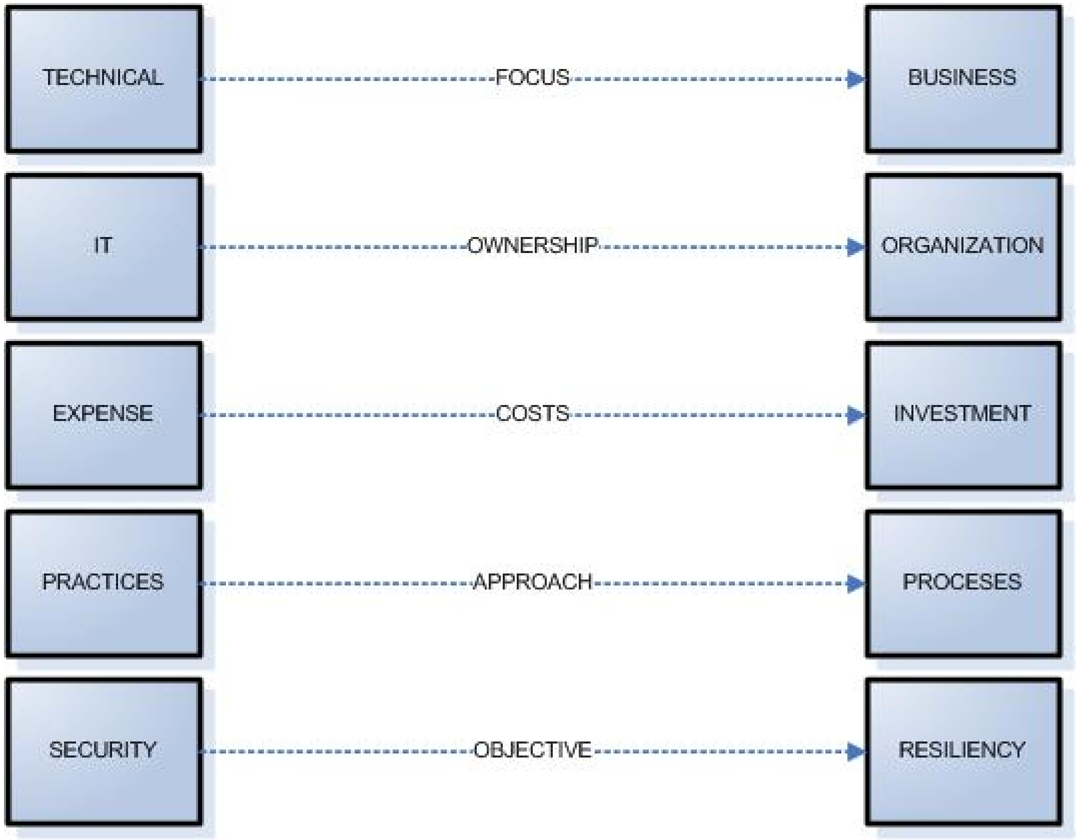
Security is an operational risk management activity

Security has two purposes:

- Prevent disruption to core business drivers
- Sustain the survivability of the organization’s mission

Security is not an end, but a means to achieving higher organizational goals

An evolving view of security -2



Operational risk and resiliency

Operational risk is the risk that results from

- Failed internal processes
- Inadvertent or deliberate actions of people
- Problems with systems and technology
- External events

Operational resiliency is the organization’s ability to sustain the mission in the face of these risks

Operational resiliency is an emergent property

Operational resiliency depends on effective management of core ORM activities

Security is one….

….but so are Business Continuity and IT Operations Management

Operational resiliency *emerges* from how well these activities are coordinated and executed toward a common goal

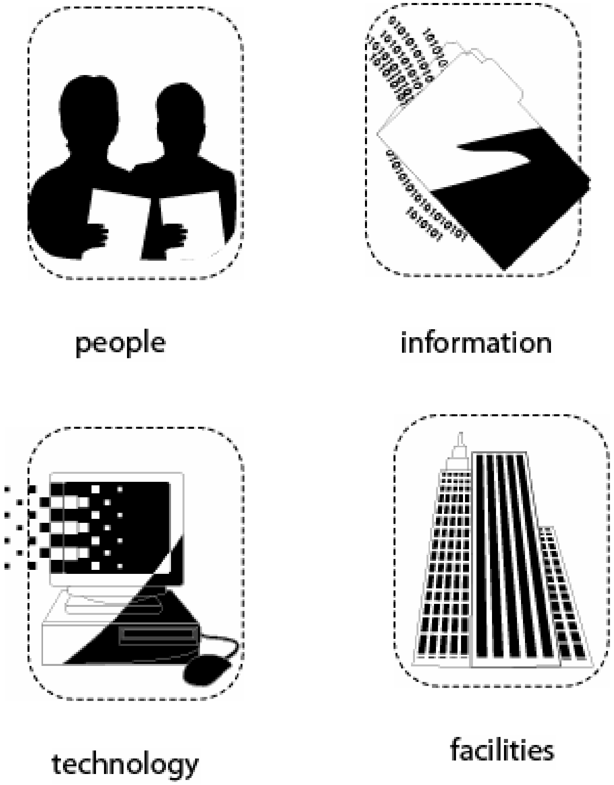
Security and operational resiliency

Focus on keeping critical assets safe from harm

Limiting threats and managing impacts

Manage confidentiality, integrity, and availability

Manage “condition”

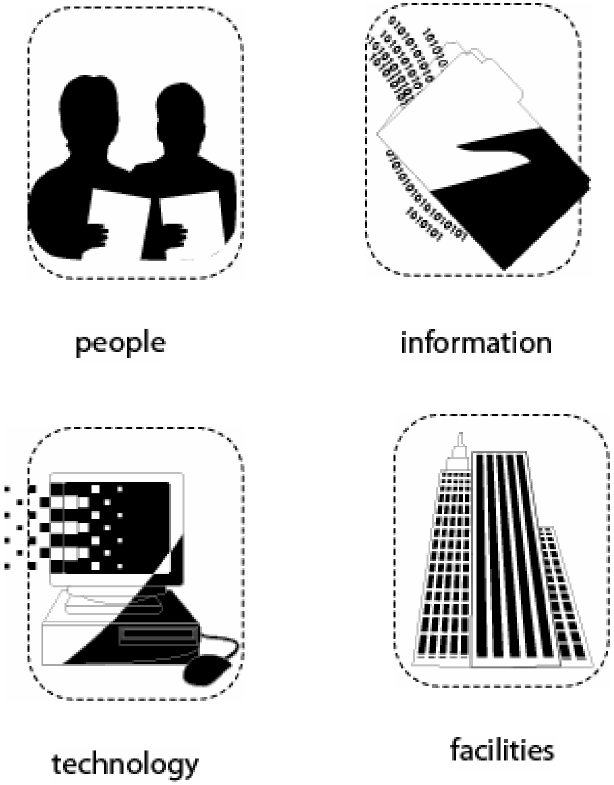


Business continuity and operational resiliency

Limit unwanted effects of realized risk

Ensure availability and recoverability

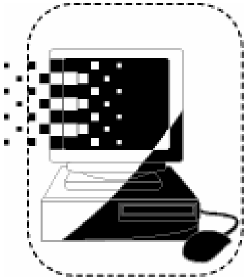
Manage “consequence”

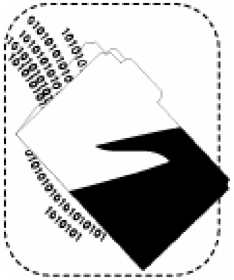


IT Operations Management and operational resiliency

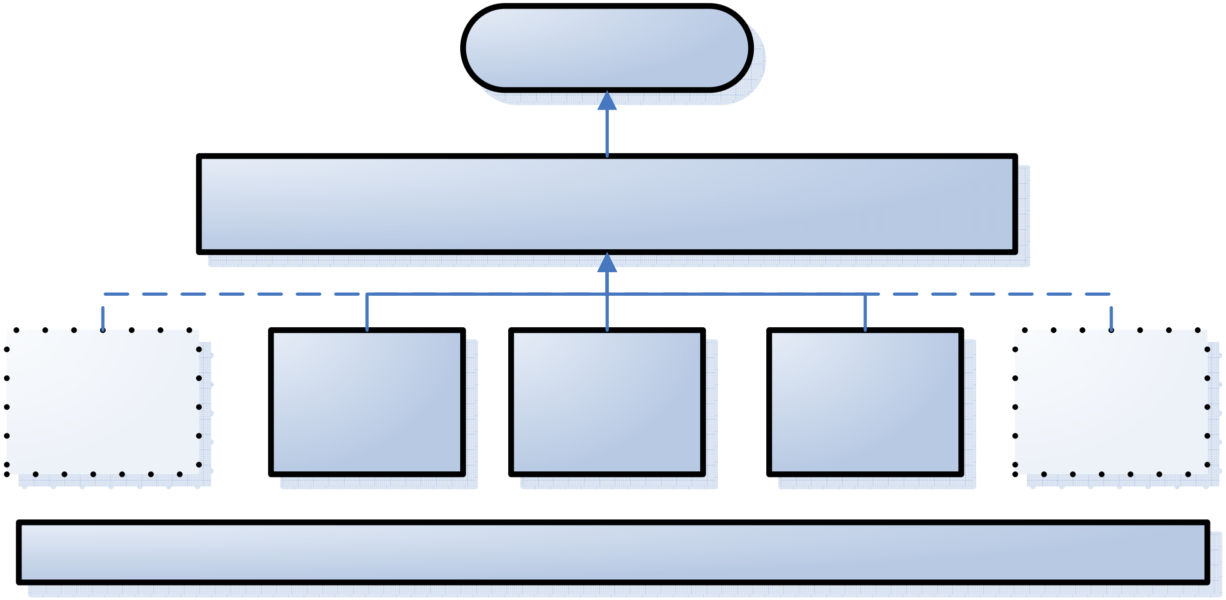
Limit vulnerabilities and threats that originate in the technical infrastructure

Ensure availability and recoverability of technology

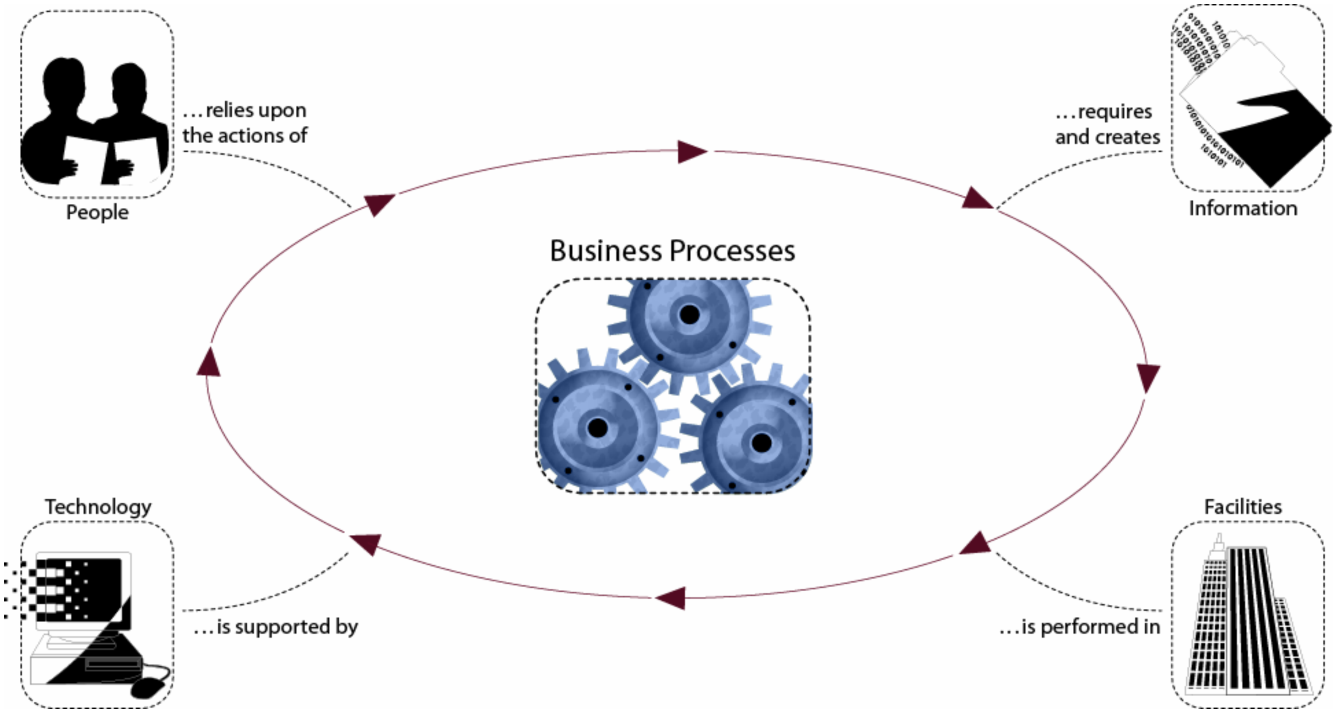

technology


information

Collaborating toward a common goal



Operational resiliency in practice

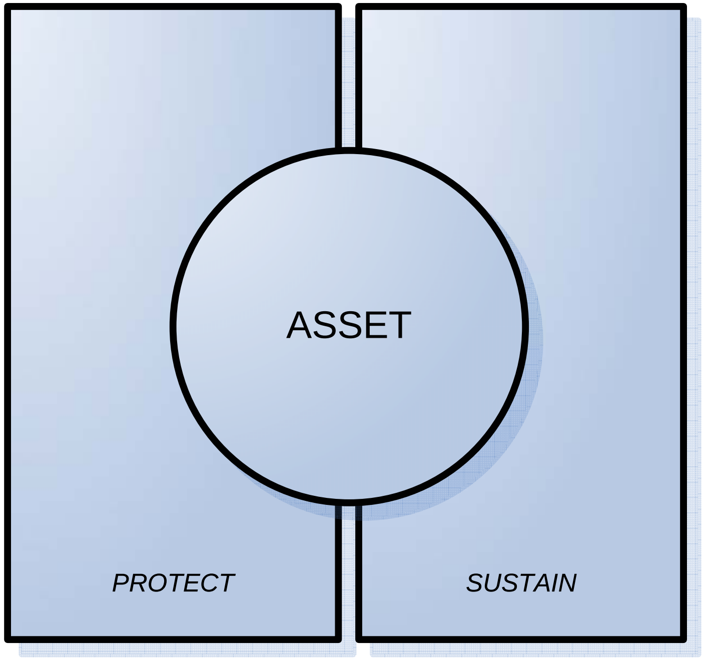


An emerging holistic view

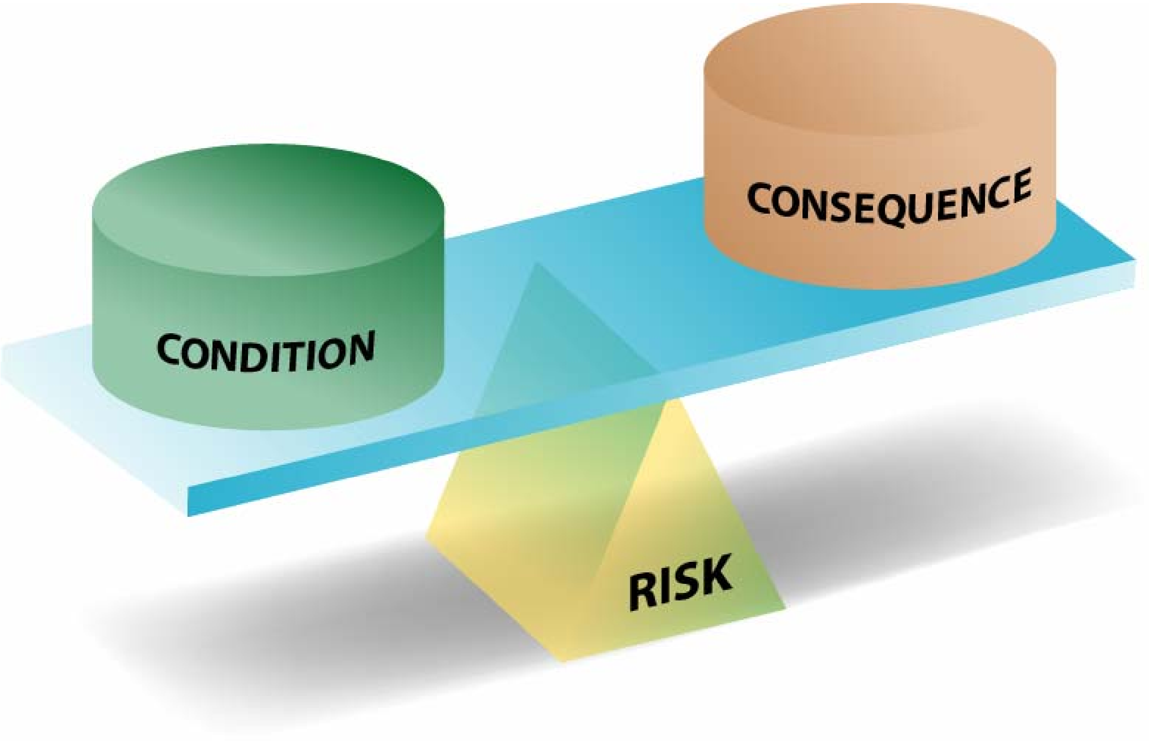
Organization is dependent on the productivity of four assets:

- People
- Information
- Technology
- Facilities

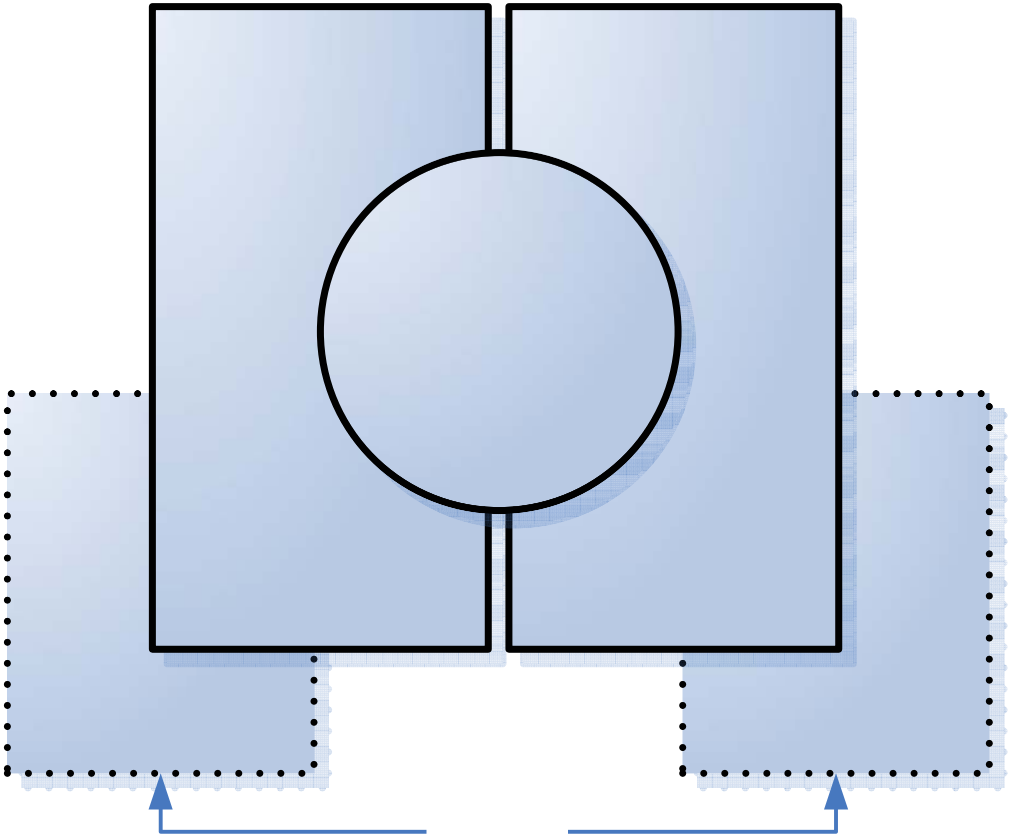
Each asset must be protected and sustainable



A holistic risk perspective

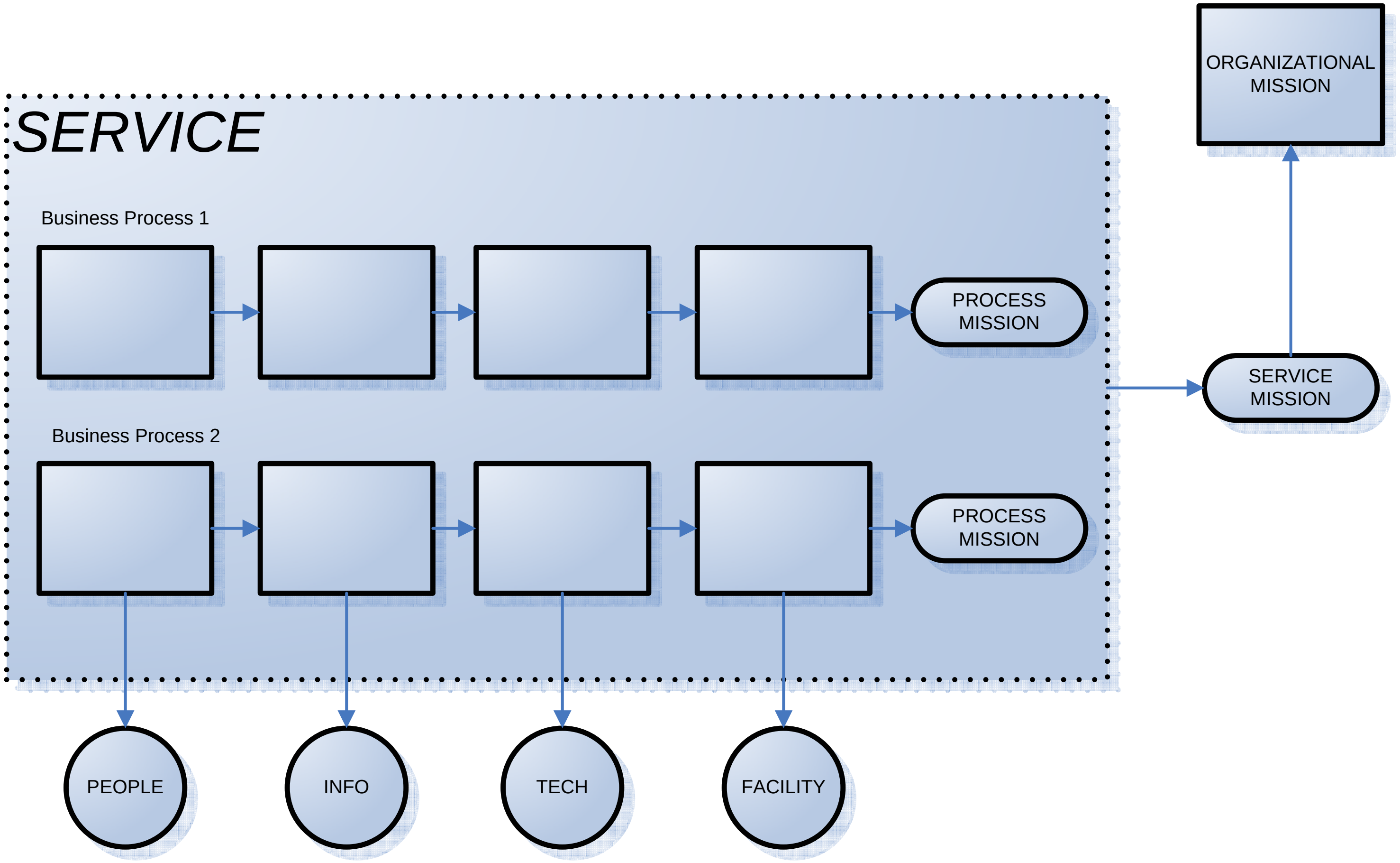


Collaborating toward a common goal



Resiliency means managing the conditions and consequences of risk balanced against business drivers and costs

A mission focus



How does an organization achieve this?

Organizations are not structured today to facilitate collaboration toward a common goal of resiliency

- Deficient funding models
- Management direction and oversight lacking
- Practice-driven
- Compliance-focused

Need to view resiliency as a definable, manageable, enterprise-wide process

CERT

Embracing a Process View of Security and Operational Resiliency

Defining a process approach

Elevating the management and coordination of operational-resiliency focused activities to the enterprise level

- Shared goals and resources
- Elimination of redundancy and stovepipes
- Elimination of framework quagmire through practice integration
- Measuring process effectiveness
- Moving toward process improvement

How does process differ from practice?

Process

- *Describes* the “what”
- Set and achieve process goals
- Manage process to requirements
- Select practices based on process goals
- Can be defined, communicated, measured, and controlled

Practice

- *Prescribes* the “how”
- No practice goals
- Tends toward “set and forget” mentality
- Reinforces domain-driven approach
- One size does not fit all
- Regulatory vehicle

The lure of best practices -1

Best practices are

- effective ways to approach improvement in a critical organizational activity, like security

Best practices ARE NOT

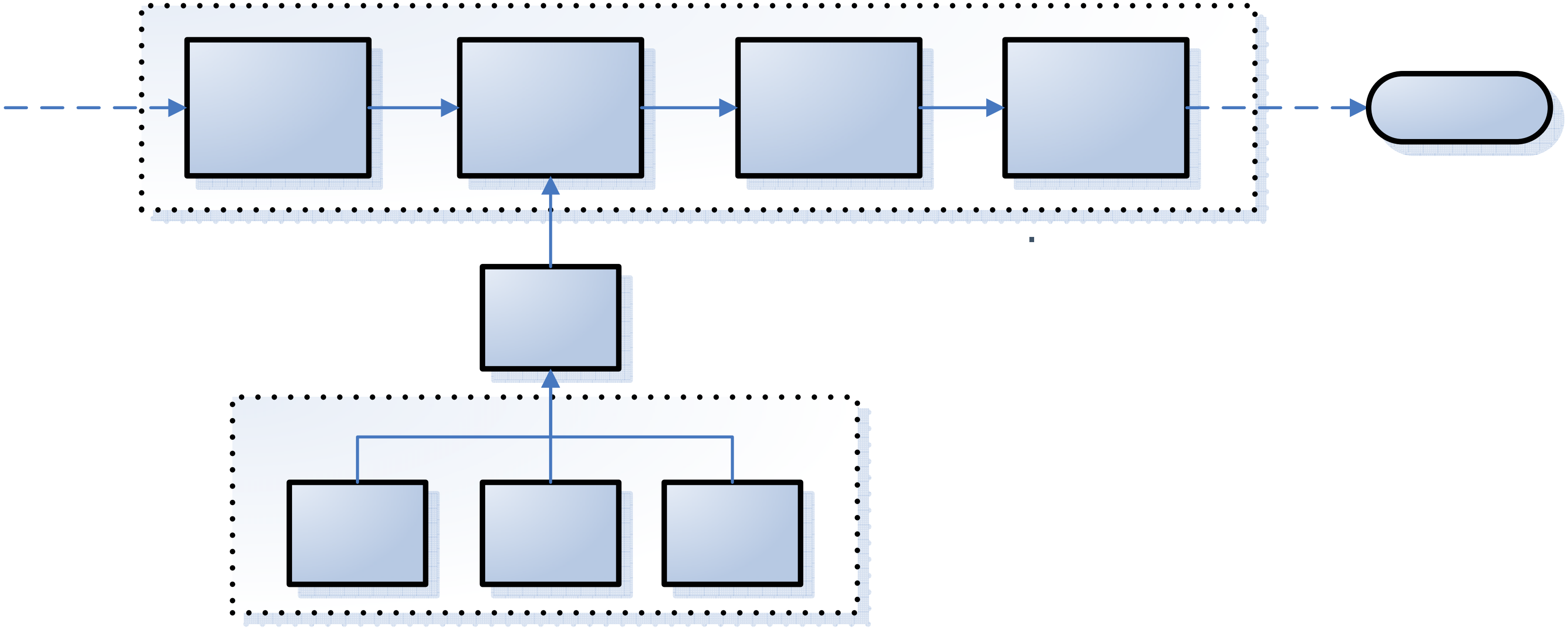
- a substitute for an actively planned and managed process

The lure of best practices -2

Best practices. . .

- Are often industry or discipline-specific
- Change/evolve frequently
- Don’t have process improvement or management aspects built-in
- Don’t provide long-term, sustainable success
- Can reinforce stove-piping and silos
- People still must implement and manage them
- Can create a management quagmire

The relationship between process and practice



Embracing process improvement

Improvement in meeting resiliency goals is dependent on the active management of the process

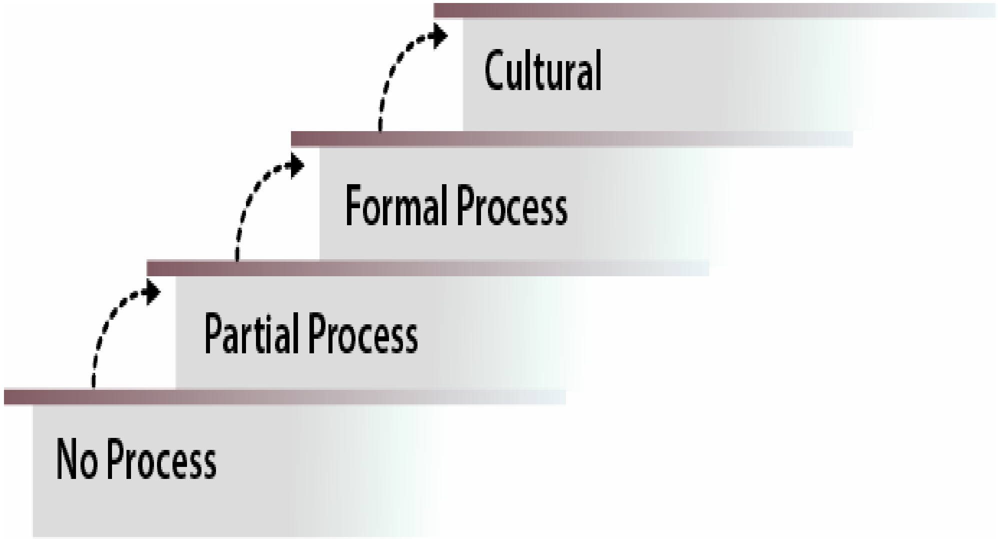
Process maturity increases capability for meeting goals and sustaining the process

"Are we resilient?" or *"Are we secure?"* is answered in the context of goal achievement rather than **what hasn't happened**

Facilitates meaningful, purposeful selection and implementation of practices

How mature are your processes?

Most organizations have some process (implicit or explicit) for resiliency engineering, but it may not be effective for meeting goals.



Thanks to www.betterproductdesign.net/maturity.htm for the generic categories.

Lack of process

No process defined or performed

Anarchy and heroics

No awareness of benefits of process-orientation

AD-HOC

Common attributes:

- Focus on events
- Ambiguous lines of responsibility
- Funding sporadic
- No alignment to strategic drivers
- Highly dependent on people
- No governance structure

Partial process

Process recognized

Still functionally focused (not enterprise-wide)

Not repeatable or actively managed

VULNERABILITY-DRIVEN

Common attributes:

- Focus on vulnerabilities
- Responsibility emanates from IT
- Considered an expense or burden
- Awareness of strategic drivers
- Still dependent on people and vul catalogs
- Informal governance

Formal process

Performed and managed

Repeatable

Spans enterprise

Not completely ingrained in culture

RISK-DRIVEN

Common attributes:

- Focus on critical assets
- Responsibility of key organizational managers and IT
- Funded as an expense
- Implicit alignment to strategic drivers
- Dependent on localized risk management
- Informal governance, possibly CRM

Cultural

Performed and managed

Repeatable and proactive

Spans and involves enterprise

Process continually measured and improving

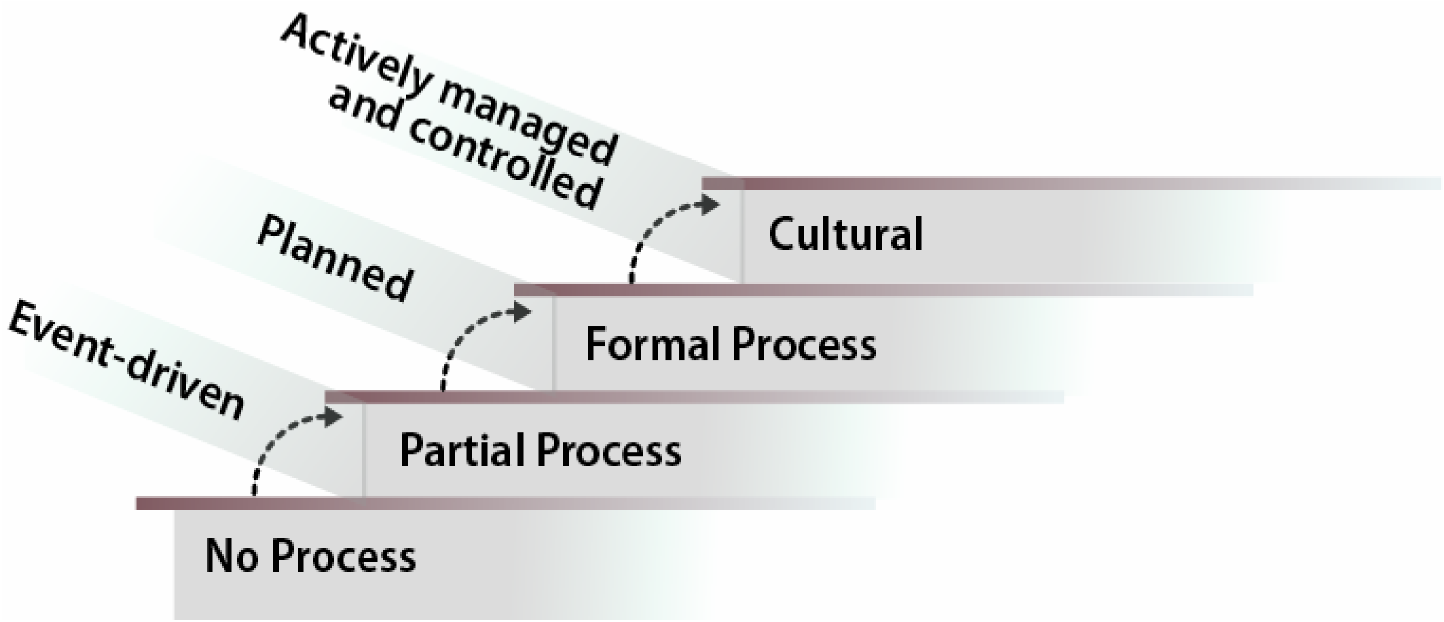
Fundamental to organizational success

ENTERPRISE-DRIVEN

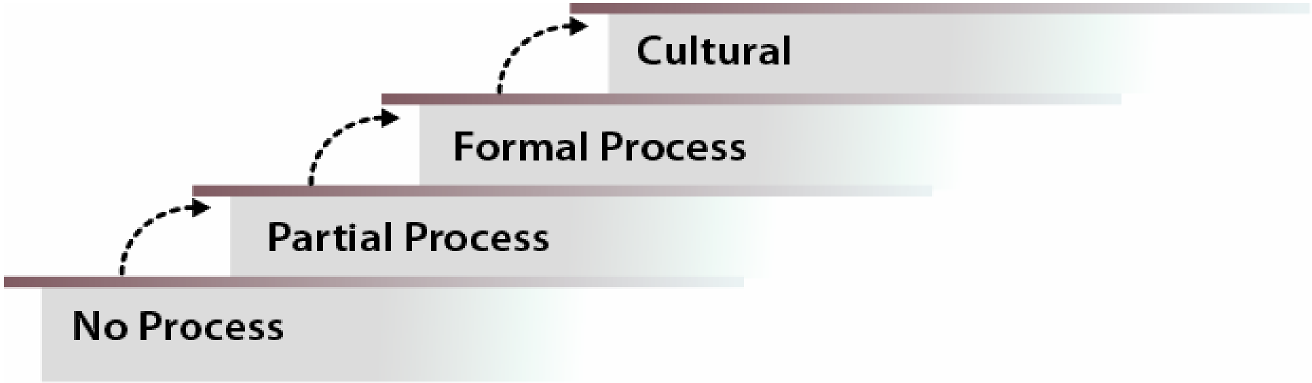
Common attributes:

- Focus on critical assets, processes, strategic drivers
- Responsibility of high-level executive
- Capitalized
- Explicit alignment to strategic drivers
- Reliant upon enterprise capabilities
- Formal governance and feedback

Increasing levels of competency



Maturity from a security perspective

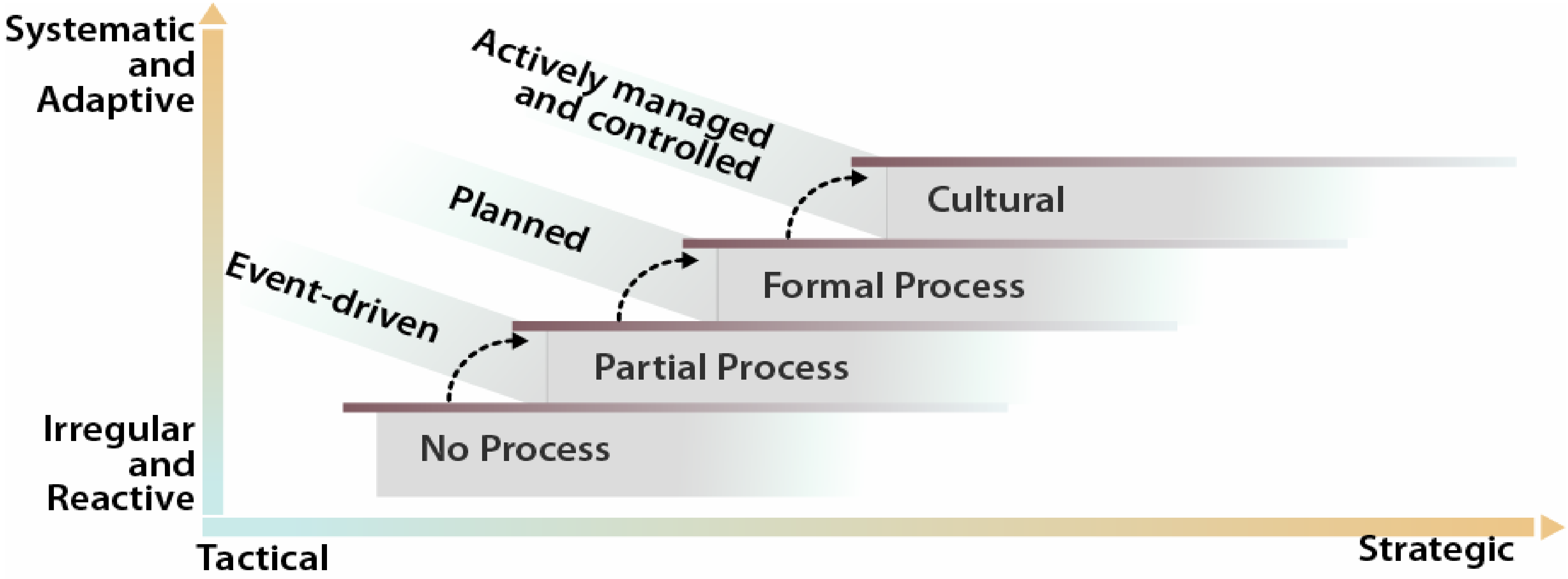


- Technical problem
- Owned by IT
- Expense-driven
- Practice-centric
- Security and survivability

→

- Business problem
- Owned by organization
- Investment-driven
- Process-centric
- Enterprise resiliency

Toward continuous improvement



Introducing the Resiliency Engineering Framework

What is resiliency engineering?

The process by which an organization establishes, develops, implements, and manages the operational resiliency of services, related business processes, and associated assets

“Requirements-driven security and business continuity”

“Building resiliency into assets/processes/services and managing to an appropriate level of adequacy”

The Resiliency Engineering Framework

A framework of practice for integration of security and business continuity activities toward achievement of operational resiliency

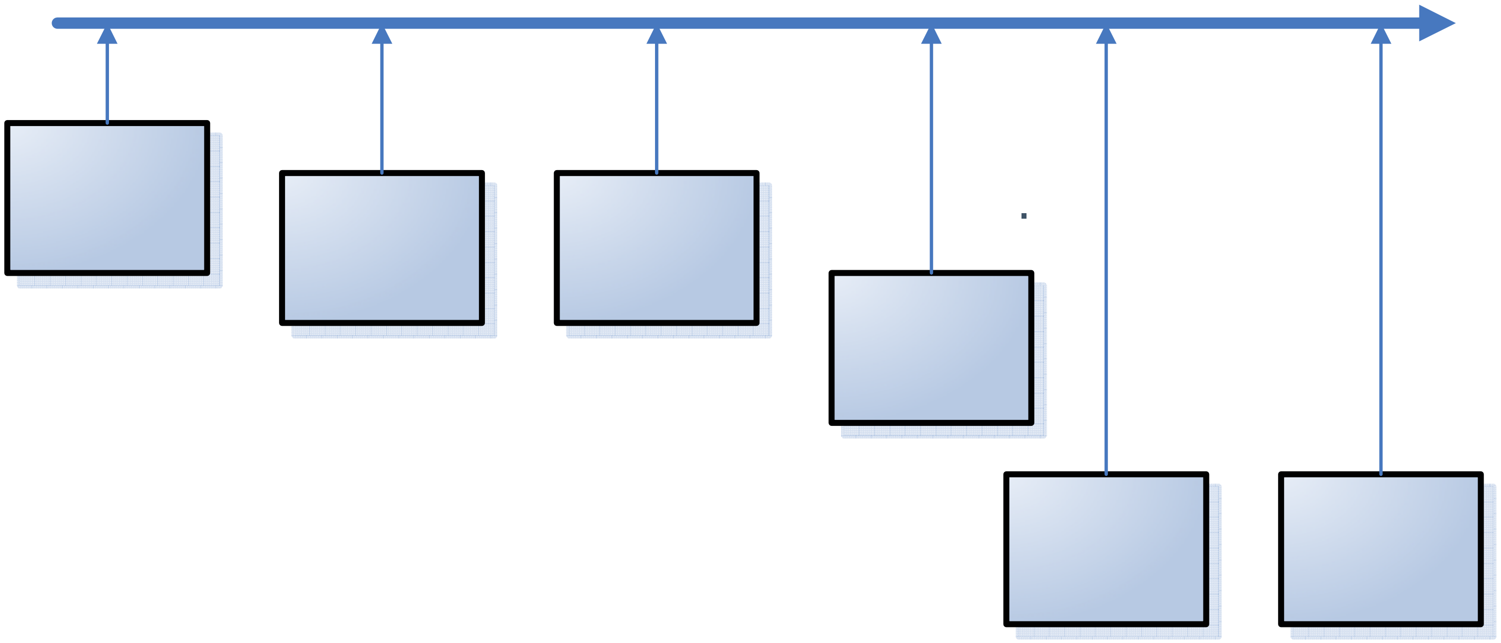
Defines basic process areas and provides guidelines for security and BC/DR process improvement

Captures vital linkages between security, BC/DR, and I/T ops in the process definition

Addresses operational risk management through process management

Establishes a capability benchmark

Project history and evolution



Development history

OCTAVE development and fieldwork

Affinity analysis of 750 practices

Identification of capabilities

Identification of processes

Development of process goals and practices

Exploration of maturity concepts

Exploration of assessment methodologies

Framework architecture

Represents processes that span four basic areas:

- Enterprise management
- Engineering
- Operations management
- Process management

Considers the resiliency of people, information, technology, and facilities in the context of services and business objectives

Enterprise management processes

Enterprise capabilities that are essential to supporting the resiliency engineering process

RSKM – Risk Management

EF – Enterprise Focus

COMP – Compliance Management

FRM – Financial Resource Management

HRM – Human Resource Management

Operations management processes

Capabilities focused on sustaining an adequate level of operational resiliency

SAM – Supplier Agreement Management

SRM – Supplier Relationship Management

AMC – Access Management and Control

IMC – Incident Management and Control

VM – Vulnerability Management

EC – Environmental Control

KIM – Knowledge and Information Management

SOM – Security Operations Management

ITOPS – IT Operations Management

Engineering processes

Capabilities focused on establishing and implementing resiliency for organizational assets, business processes, and services

RD – Requirements Definition

RM – Requirements Management

AM – Asset Management

COOP – Continuity of Operations Planning

REST – Restoration of Operations Planning

CSI – Control Selection and Implementation

RAD – Resilient Architecture Development

Process management processes

Enterprise capabilities related to defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving processes

OT – Organizational Training

OPF – Organizational Process Focus

OPD – Organizational Process Definition

MA – Measurement and Analysis

MON - Monitoring

Using the framework

Establish current level of capability

Set forward-looking resiliency goals and targets

Develop plans to close identified gaps

Build resiliency into important assets/processes/services and architectures

Reduce reactionary activities; shift to directing and controlling activities

Align common practices with processes to achieve process goals

Collaborating with industry

Eighteen month collaboration with Financial Services Technology Consortium

Identify mature practices in mature industries: banking and financial services

Two phases of work—capability identification and process definition

Financial Services Technology Consortium

Established in 1993

Member-owned consortium for collaboration between financial services-focused organization

Explore new technologies and methodologies to address today’s business requirements

Projects:

- Technology Review
- Compliance
- Business Continuity Maturity Model

FSTC Project Members

Ameriprise

Bank of America

Carnegie Mellon

Capital Group

Citicorp

Discover

DRII

DRJ

IBM

JPMorgan Chase

Key Bank

KPMG

MasterCard

Marshall and Ilsley

NY Federal Reserve Bank

SunGard

Trizec Properties

US Bank

Wachovia

Where do we go from here?

Release REF v0.9 in October 2006 for comments

Establish guidelines for improving the security and business continuity processes

Phase III expansion of model development and piloting

Exploration of integration with other existing models

Development of appraisal methodology to measure capability for managing resiliency

Summary and questions

Operational resiliency must be actively managed

Security, BC/DR, and IT Ops must collaborate

Model-based process improvement brings defined, systematic, repeatable, consistent, and improvable processes

Approach must be flexible and adaptable

No one-size-fits-all solution

Contact Us

Speakers
Richard Caralli **rcaralli@cert.org**

Lisa Young **lry@sei.cmu.edu**

Phone
412-268-5800
(8:30 a.m. - 4:30 p.m. EST)

Web
http://www.cert.org
http://www.cert.org/nav/index_green.html

Postal Mail
Software Engineering Institute
ATTN: Customer Relations
Carnegie Mellon University
Pittsburgh, PA 15213-3890